

Normalizers of Congruence Groups in $SL_2(\mathbb{R})$ and Automorphisms of Lattices

Shaul Zemel

December 24, 2015

Introduction

If Γ is a congruence subgroup of $SL_2(\mathbb{Z})$ then there are several reasons to study the normalizer of Γ in $SL_2(\mathbb{R})$. The main motivation is, except pure interest, that the quotient of that normalizer modulo Γ embeds (under some assumptions on elliptic points) into the group of automorphisms of the Riemann surface X_Γ associated with Γ . Moreover, elements of this normalizer act on spaces of modular forms with respect to Γ , endowing these already rich spaces with additional structure.

For the most classical congruence groups, namely $\Gamma_0(N)$ for natural N , many references describe this normalizer (see, e.g., [LN] or Section 3 of [CN], while [N1] restricts attention to the normalizer in $SL_2(\mathbb{Z})$ itself, which is very easily determined as $\Gamma_0(\frac{N}{\sigma})$ where σ is the largest divisor of 24 whose square divides N), as well as the quotient modulo $\Gamma_0(N)$. This quotient is a very simple group if the powers of 2 and 3 which divide N are very small, but otherwise it gets significantly more complicated (see [AL] for the first results on that quotient, though [AS] and [B] later corrected some errors in that reference, and also related it to automorphisms of the modular curve $X_0(N)$). We mention [N2] for some general results on normalizers of congruence subgroups of $SL_t(\mathbb{Z})$ inside $SL_t(\mathbb{R})$ for any $t \geq 2$.

A tool which many of these references use is the Big Picture Ω , first defined in [C], which is a certain graph whose vertices are the finitely generated subgroups of full rank in \mathbb{Q}^2 modulo homothety, with edges according to an explicit rule. [L1] uses it in order to determine the normalizer of the image of $\Gamma_1(N)$ inside $PSL_2(\mathbb{R})$, and it also appears in the construction of the algorithm, developed in [L3], for determining normalizers of general subgroups (after one finds generators for the subgroup). We mention that [L2] is concerned with the normalizers of groups which are slightly larger than $\Gamma_0(N)$, and not contained in $SL_2(\mathbb{Z})$, and uses it for finding normalizers of certain subgroups of the Hecke groups G_4 and G_6 .

The aim of this paper is to give an present the normalizers of various families of congruence groups, which are much more general than just $\Gamma_0(N)$ and $\Gamma_1(N)$.

The main groups we investigate lie between these two groups, so that any such group is associated to a unique subgroup H of $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. We begin by introducing a group, which we denote by $\Gamma_0^{*,sN}(N)$, containing $\Gamma_0(N)$ with finite index, in which all these normalizers are contained, and then give conditions on elements of $\Gamma_0^{*,sN}(N)$ which are equivalent to normalizing the subgroup which is associated with H . Using these conditions we write the normalizer explicitly for two types of subgroups H , namely the kernel of the projection to $(\mathbb{Z}/D\mathbb{Z})^\times$ (i.e., the normalizers of the intersection $\Gamma_0(N) \cap \Gamma_1(D)$) for some divisor D of N and the m -torsion subgroups for divisors m of the exponent $\lambda(N)$ of $(\mathbb{Z}/D\mathbb{Z})^\times$, together with some additional results.

In addition, some lattices of signature $(2, 1)$ have discriminant kernels which are (isomorphic to) congruence subgroups—see, e.g., [LZ], or [BO] and the references therein, among others. The lattices appearing in these references are related to $\Gamma_1(N)$ and $\Gamma_0(N)$ respectively, and they are also part of a larger family of lattices $L(N, D)$, whose discriminant kernels turn out to be congruence subgroups as well. The automorphism groups of such a lattice is contained in the normalizer of its discriminant kernel, a simple observation which links the two questions to one another. We also present these lattices $L(N, D)$, and show how the tools developed for determining normalizers can also be used for finding the automorphism group of $L(N, D)$ and its discriminant kernel.

We remark that we are only interested in the normalizers themselves, not in the structure of the quotient modulo the congruence group. This is so, since this quotient is complicated in general: See the case of $\Gamma_0(N)$ considered in [AS] and [B], or the case of $\Gamma_1(N)$, where Corollary 3.2 shows that this group is an extension of $\{\pm 1\}^{\{p|N\}}$ by $(\mathbb{Z}/N\mathbb{Z})^\times$. As the action of the former group on the latter is, in general, non-trivial (it is described explicitly in Proposition 2.7), and the extension is non-trivial, we leave the questions about the structure of the quotient for further research.

This paper is divided into 4 sections. In Section 1 we introduce the group $\Gamma_0^{*,sN}(N)$ and some of its important subgroups, and proves some of their properties. In Section 2 we establish the tool for determining the normalizer of any intermediate group between $\Gamma_1(N)$ and $\Gamma_0(N)$. Section 3 describes the normalizers of several families of subgroups, in particular $\Gamma_0(N) \cap \Gamma_1(D)$ for $D|N$ and the subgroups associates with m -torsion in $(\mathbb{Z}/N\mathbb{Z})^\times$. Finally, Section 4 presents the lattices $L(N, D)$ and calculates their automorphism groups as well as their discriminant kernels.

1 Some Matrix Groups

In this Section we present some types of groups, which will appear as normalizers of congruence subgroups below. We recall that $\Gamma_0(N)$, where N is any positive integer, is the group consisting of those matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ such that $N|c$, and that $\Gamma_1(N)$ is the subgroup of $\Gamma_0(N)$ in elements of which the diagonal entries a and d are congruent to 1 modulo N . In addition, $\Gamma^0(N)$ is the subgroup of $SL_2(\mathbb{Z})$ on elements of which we impose the condition $N|b$, and $\Gamma^1(N)$ is

obtained from $\Gamma^0(N)$ in the same way as one defines $\Gamma_1(N)$ in $\Gamma_0(N)$. If M and N are two positive integers then $\Gamma_0^0(N, M)$, $\Gamma_1^0(N, M)$, and $\Gamma_0^1(N, M)$ are the intersections $\Gamma_0(N) \cap \Gamma^0(M)$, $\Gamma_1(N) \cap \Gamma^0(M)$, and $\Gamma_0(N) \cap \Gamma^1(M)$ respectively. The intersections $\Gamma_1^0(N, N)$ and $\Gamma_0^1(N, N)$ yield the principal congruence subgroup $\Gamma(N)$, which is the kernel of the (surjective) group homomorphism from $SL_2(\mathbb{Z})$ to $SL_2(\mathbb{Z}/N\mathbb{Z})$.

Given any positive integer M , we define s_M to be the square root of its square part, and t_M is the “remainder”. This means that s_M and t_M are the unique positive integers such that $M = s_M^2 t_M$ with t_M square-free. In addition, for a prime number p and an integer M , we denote the maximal integer k such that $p^k | M$ by $v_p(M)$ (the p -adic valuation of M). A divisor μ of an integer N is called *exact* if it is co-prime to $\frac{N}{\mu}$.

Definition 1.1. Let $\Gamma_0^{*,sN}(N)$ be the set of matrices $A \in M_2(\mathbb{R})$ which admit a presentation of the form $\begin{pmatrix} a\sqrt{\mu} & b/\sqrt{\mu} \\ c\frac{N}{\mu}\sqrt{\mu} & d\sqrt{\mu} \end{pmatrix}$, where μ is an exact divisor of N , a and d are in $\frac{1}{s_\mu}\mathbb{Z}$, and b and c are in $\frac{1}{s_{N/\mu}}\mathbb{Z}$, such that the equality $ad\mu - bc\frac{N}{\mu} = 1$ is satisfied.

The latter equality in Definition 1.1, which is a difference between two integers by our assumptions of a , b , c , and d , is equivalent to $\Gamma_0^{*,sN}(N)$ being a subset of $SL_2(\mathbb{R})$. The properties of $\Gamma_0^{*,sN}(N)$ which will be of interest to us are the following ones.

Proposition 1.2. (i) $\Gamma_0^{*,sN}(N)$ is a subgroup of $SL_2(\mathbb{R})$.

(ii) Conjugation from $\Gamma_0^{*,sN}(N)$ takes $\Gamma_1(N)$ into $\Gamma_0(N)$.

Proof. We first observe that $\Gamma_0^{*,sN}(N)$ is stable under inversion of elements of $SL_2(\mathbb{R})$. For evaluating the product of the matrix appearing in Definition 1.1 with another such matrix, say $\begin{pmatrix} e\sqrt{\nu} & f/\sqrt{\nu} \\ g\frac{N}{\nu}\sqrt{\nu} & h\sqrt{\nu} \end{pmatrix}$, we define $\delta = (\mu, \nu)$ and $\kappa = \frac{\mu\nu}{\delta^2}$. Then κ is an exact divisor of N , and the product in question equals

$$\begin{pmatrix} (ae\delta + bg\frac{N}{\delta\kappa})\sqrt{\kappa} & (af\frac{\mu}{\delta} + bh\frac{\nu}{\delta})/\sqrt{\kappa} \\ (ce\frac{\nu}{\delta} + dg\frac{\mu}{\delta})\frac{N}{\kappa}\sqrt{\kappa} & (cf\frac{N}{\delta\kappa} + dh\delta)\sqrt{\kappa} \end{pmatrix}. \quad (1)$$

As $s_\mu a$, $s_\mu d$, $s_{N/\mu} b$, $s_{N/\mu} c$, $s_\nu e$, $s_\nu h$, $s_{N/\nu} f$, and $s_{N/\nu} g$ are integers, it is easy to verify that multiplying the expressions appearing in parentheses in the diagonal entries of the matrix from Equation (1) by s_κ and the ones appearing in the off-diagonal entries by $s_{N/\kappa}$ yield integral values as well. Hence the product also satisfies the conditions of Definition 1.1, establishing part (i).

For part (ii) we observe that conjugating any matrix $\gamma = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in M_2(\mathbb{R})$ by the matrix A from Definition 1.1 yields

$$\begin{pmatrix} bdg - acfN + ade\mu - bch\frac{N}{\mu} & a^2f\mu - ab(e - h) - b^2\frac{g}{\mu} \\ d^2g\mu + cdN(e - h) - c^2f\frac{N^2}{\mu} & acfN - bdg + adh\mu - bce\frac{N}{\mu} \end{pmatrix}. \quad (2)$$

Hence if $\gamma \in \Gamma_1(N)$ then the conditions on a , b , c , and d in Definition 1.1 combine with the fact that $\frac{g}{N}$, $\frac{e-h}{N}$, and f are integers to show that the conjugated matrix

$A\gamma A^{-1}$ lies in $\Gamma_0(N)$. This proves the part (ii), which completes the proof of the proposition. \square

Regarding the uniqueness and normalization of the presentation from Definition 1.1, we obtain the following corollary.

Corollary 1.3. *Let A be an element of $\Gamma_0^{*,s_N}(N)$, presented as in Definition 1.1, and let p be a prime dividing N .*

- (i) *If $v_p(N)$ is odd (i.e., $p|t_N$) then p divides either $ad\mu$ or $bc\frac{N}{\mu}$ (according to whether p divides μ or $\frac{N}{\mu}$).*
- (ii) *If $v_p(N)$ is even then one may transfer $p^{v_p(s_N)}$ between μ and $\frac{N}{\mu}$ and obtain a different presentation.*

Proof. If $v_p(N)$ is odd and $p|\mu$ (resp. $p|\frac{N}{\mu}$) then the powers of p in the denominators of a and d (resp. b and c) can cancel at most a power of $2v_p(s_N) = v_p(N) - 1$ from the expression $p^{v_p(N)}$ appearing in μ (resp. $p|\frac{N}{\mu}$). This proves part (i). For part (ii), note that if $\mu = p^{2v_p(s_N)}\nu$ then the matrix A from Definition 1.1 can also be written as $\begin{pmatrix} ap^{v_p(s_N)}\sqrt{\nu} & (b/p^{v_p(s_N)})/\sqrt{\nu} \\ (c/p^{v_p(s_N)})\frac{N}{\nu}\sqrt{\nu} & dp^{v_p(s_N)}\sqrt{\nu} \end{pmatrix}$, while in case p divides $\frac{N}{\mu}$ to an even power $2v_p(s_N)$ then it can take the form $\begin{pmatrix} (a/p^{v_p(s_N)})\sqrt{\nu} & bp^{v_p(s_N)}/\sqrt{\nu} \\ cp^{v_p(s_N)}\frac{N}{\nu}\sqrt{\nu} & (d/p^{v_p(s_N)})\sqrt{\nu} \end{pmatrix}$. As the new rational coordinates have the required bounded denominators, this proves the corollary. \square

Of the several presentations an element of $\Gamma_0^{*,s_N}(N)$ was seen in Corollary 1.3 to have, some presentations are more convenient than others.

Lemma 1.4. (i) *The two summands from the SL_2 equality in Definition 1.1, as well as the four products ab , ac , bd , and cd , are independent of the presentation.*

- (ii) *Any element of $\Gamma_0^{*,s_N}(N)$ has at least one presentation in which the four products from part (i) involve no cancelations.*

Proof. Part (i) is clear from the explicit formulae for the presentation changes in the proof of Corollary 1.3 (or from the fact that the asserted expressions are, up to multiplication by N , products of two of the entries of the matrix itself). Now, the conditions from Definition 1.1 show that only cancelations of primes p dividing N have to be considered. Assuming that $p|\mu$, cancelation in powers of p may only occur if p divides the numerators of either b or c . But then the number $bc\frac{N}{\mu}$ would be divisible by p , so that $ad\mu$ will be prime to p (since their difference is 1). This can only happen if $v_p(N)$ is even and both a and d have the full power $p^{v_p(s_N)}$ in their denominators. But then applying Corollary 1.3 to use the divisor $\nu = \mu/p^{v_p(N)}$ would give a form in which the numbers in the off-diagonal entries may have p -powers in their denominators but the numerators of the new numbers in the diagonal entries are not divisible by p . The case

where $p \mid \frac{N}{\mu}$ is established by the same argument, interchanging the roles of the diagonal and off-diagonal elements, and using the divisor $p^{v_p(N)}\mu$ instead. This established part (ii), hence proves the lemma. \square

Remark 1.5. The proof of Lemma 1.4 shows that a presentation involves cancellations in a prime $p \mid N$ only in case one of the summands from Corollary 1.3 is divisible by p but we take the power of p to be in the divisor (μ of $\frac{N}{\mu}$) which is associated with the other summand. Part (ii) of Lemma 1.4 allows us to avoid such presentations. A presentation as in part (ii) of Lemma 1.4 is also in line with the fact that for primes dividing t_N , the summand corresponding to the divisor of N which is divisible by p is also divisible by p .

We shall make use of another simple lemma.

Lemma 1.6. (i) *The operation sending μ and ν of N to κ in the proof of Proposition 1.2 defines a group structure on the set of exact divisors of N , making it a group which is isomorphic to $\{\pm 1\}^{\{p \mid N\}}$.*

(ii) *For any divisor $D \mid N$, there exists a canonical projection from $\{\pm 1\}^{\{p \mid N\}}$ to $\{\pm 1\}^{\{p \mid D\}}$, which is surjective and its kernel consists of all the exact divisors μ of N which are co-prime to D .*

Note that the interpretation of $\{\pm 1\}^{\{p \mid D\}}$ as a quotient of $\{\pm 1\}^{\{p \mid N\}}$ in part (ii) of Lemma 1.6 is *not* based on exact divisors of D , a set which also produces a group isomorphic to $\{\pm 1\}^{\{p \mid D\}}$ by part (i) of that lemma.

Proof. It is clear from the definition that $\mu = \prod_{p \mid \mu} p^{v_p(N)}$ and $\nu = \prod_{p \mid \nu} p^{v_p(N)}$ then κ is the product of $p^{v_p(N)}$ over all the primes dividing μ or ν but not both. This proves part (i). For part (ii) the map taking the component of $p \mid D$ to itself and the component of $p \mid N$ which does not divide D to the trivial element is clearly well-defined and surjective, and the translation to divisors of N immediately yields the desired assertion. This proves the lemma. \square

We generalize Definition 1.1 as follows.

Definition 1.7. Let σ be any divisor of s_N . Then we define $\Gamma_0^{*,\sigma}(N)$ to be the set of elements of $\Gamma_0^{*,s_N}(N)$ for which the power of p dividing any of the denominators of a , b , c , and d in a presentation as in Definition 1.1 which satisfies the conditions of Lemma 1.4 is at most $v_p(\sigma)$. In particular, the group $\Gamma_0^*(N) = \Gamma_0^{*,1}(N)$, in elements of which a , b , c , and d are integers, is the group obtained from $\Gamma_0(N)$ by adding the *Atkin-Lehner involutions*.

Remark 1.8. Lemma 1.4 shows that the condition of Definition 1.7 is satisfied if and only if σab and σcd , or equivalently σac and σbd , are integral. Part (i) of Lemma 1.3 shows that these equivalent characterizations of elements of $\Gamma_0^{*,\sigma}(N)$ are satisfied also in presentations which may not satisfy the conditions of Lemma 1.4.

Proposition 1.9. (i) The set $\Gamma_0^{*,\sigma}(N)$ from Definition 1.7 is a subgroup of $\Gamma_0^{*,sN}(N)$, which contains $\Gamma_0(N)$.

(ii) Two different presentations elements of $\Gamma_0^{*,\sigma}(N)$, both of which satisfy the conditions of Lemma 1.4, may arise only from operations using primes $p|N$ which do not divide $\frac{N}{\sigma^2}$.

(iii) The index $[\Gamma_0^{*,\sigma}(N) : \Gamma_0(N)]$ is $\sigma^2 \prod_{p|\sigma, v_p(N)=2v_p(\sigma)} (1 + \frac{1}{p}) \cdot \prod_{p|N/\sigma^2} 2$.

Proof. It is clear that $\Gamma_0^{*,\sigma}(N)$ is closed under inversion. Consider now the formula for the product of two elements appearing in Equation (1), and assume that the two multipliers lie in $\Gamma_0^{*,\sigma}(N)$ and are presented as in Lemma 1.4. Then the same argument as in the proof of Proposition 1.2, but with replacing any number s_M by $\gcd\{s_M, \sigma\}$, establishes part (i) since the containment $\Gamma_0(N) \subseteq \Gamma_0^{*,\sigma}(N)$ is obvious. Alternatively, one may prove this part by considering the expressions from Remark 1.7 in the formula for the product appearing in Equation (1). Part (ii) follows from Remark 1.5, since the only case where a prime can divide μ but not $ad\mu$, or $\frac{N}{\mu}$ but not $bc\frac{N}{\mu}$, in an element of $\Gamma_0^{*,\sigma}(N)$ is when $2v_p(\gcd\{s_\mu, \sigma\}) = v_p(N)$ or $2v_p(\gcd\{s_{N/\mu}, \sigma\}) = v_p(N)$, i.e., when $2v_p(\sigma) = v_p(N)$.

For part (iii), first note that part (ii) shows that the map taking an element $A \in \Gamma_0^{*,\sigma}(N)$ to the divisor μ of N appearing in a presentation satisfying the conditions of Lemma 1.4 is well-defined up to at most the kernel of the map from $\{\pm 1\}^{\{p|N\}}$ to $\{\pm 1\}^{\{p|N/\sigma^2\}}$ described in part (ii) of Lemma 1.6. By parts (i) and (ii) of that Lemma, the formula for the product in Equation (1) shows that $\Gamma_0^{*,\sigma}(N)$ admits a well-defined group homomorphism to $\{\pm 1\}^{\{p|N/\sigma^2\}}$, which is clearly surjective. Moreover, the kernel of this map consists precisely of those matrices which admit a presentation as in Lemma 1.4 with $\mu = 1$. Now, the formula from Definition 1.1 and the condition from Definition 1.7 show that the matrix $\frac{1}{\sqrt{\sigma}} \begin{pmatrix} \sigma & 0 \\ 0 & 1 \end{pmatrix}$ conjugates this kernel to $\Gamma_0(\frac{N}{\sigma^2})$, while its subgroup $\Gamma_0(N)$ is taken to $\Gamma_0^0(\frac{N}{\sigma}, \sigma)$ by this operation. We thus have to compare the indices of these congruence subgroups in $SL_2(\mathbb{Z})$. But it is known (see, e.g., Section 1.2 of [DS]) that the index any group of the form $\Gamma_0(M)$ in $SL_2(\mathbb{Z})$ is $M \prod_{p|M} (1 + \frac{1}{p})$, and working modulo the principal congruence subgroup $\Gamma(M)$ we see that a subgroup of the form $\Gamma_0^0(M, D)$ with $D|M$ has index D in $\Gamma_0(M)$. Hence the index of our conjugate of $\Gamma_0(N)$ is the same index $N \prod_{p|N} (1 + \frac{1}{p})$ as for $\Gamma_0(N)$ itself in $SL_2(\mathbb{Z})$ (recall that $\sigma|s_N$, so that the prime divisors of $\frac{N}{\sigma}$ coincide with those of N), while the conjugate of our kernel has index $\frac{N}{\sigma^2} \prod_{p|N/\sigma^2} (1 + \frac{1}{p})$. Taking the quotient between these indices, noting that the sets of primes differ precisely by the ones appearing above, and multiplying by the cardinality of $\{\pm 1\}^{\{p|N/\sigma^2\}}$ (to go from the index of $\Gamma_0(N)$ in the kernel to the index in $\Gamma_0^{*,\sigma}(N)$ itself), yield the asserted value of the index. This completes the proof of the proposition. \square

Remark 1.10. The proof of part (iii) in Proposition 1.9 used the conjugation of the kernel appearing there by the matrix $\frac{1}{\sqrt{\sigma}} \begin{pmatrix} \sigma & 0 \\ 0 & 1 \end{pmatrix}$. Extending the conjugation

to all of $\Gamma_0^{*,\sigma}(N)$ yields the Atkin–Lehner group $\Gamma_0^*\left(\frac{N}{\sigma^2}\right)$, with no fractions. Moreover, the map from $\Gamma_0^{*,\sigma}(N)$ to the quotient $\{\pm 1\}^{\{p|N/\sigma^2\}}$ of $\{\pm 1\}^{\{p|N\}}$ as in part (ii) of Lemma 1.6 and the one from $\Gamma_0^*\left(\frac{N}{\sigma^2}\right)$ to $\{\pm 1\}^{\{p|N/\sigma^2\}}$ based on exact divisors of $\frac{N}{\sigma^2}$ commute with this conjugation. This is the reason for the notation used by [CN] and others for $\Gamma_0^{*,\sigma}(N)$, for σ (denoted by h in that reference) being the value appearing in Corollary 3.2. However, we shall stick to our $\Gamma_0^{*,\sigma}(N)$, since these groups, rather than their conjugates $\Gamma_0^*\left(\frac{N}{\sigma^2}\right)$, are the ones appearing as normalizers below.

2 Determining Normalizers

The intermediate groups between $\Gamma_1(N)$ and $\Gamma_0(N)$ are in correspondence with the subgroups of the quotient group $(\mathbb{Z}/N\mathbb{Z})^\times$. We denote Γ_H the intermediate group which corresponds to the subgroup $H \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$. In this Section we establish criteria for determining the normalizer of Γ_H in general. This results will be used for describing the normalizer of Γ_H for particular types of subgroups H explicitly in the following section.

We begin by considering elements $A \in SL_2(\mathbb{R})$ such that the corresponding conjugate $A\Gamma_1(N)A^{-1}$ of $\Gamma_0(N)$ is contained in $\Gamma_0(N)$. It is clear that if A normalizes some Γ_H then it has this property. Now, part (ii) of Proposition 1.2 shows that elements of $\Gamma_0^{*,sN}(N)$ do this. We would like to show that they are the only ones. The first step is given in the following lemma.

Lemma 2.1. *Assume that conjugation by a matrix $A = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in SL_2(\mathbb{R})$ takes $\Gamma_1(N)$ into $\Gamma_0(N)$. Then the expressions e^2 , eg , $\frac{g^2}{N}$, $2Nef$, $N(eh + fg)$, $2gh$, Nf^2 , Nfh , and h^2 are all integral.*

Proof. We consider only the three elements $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}$, and $\begin{pmatrix} 1+N & -N \\ N & 1-N \end{pmatrix}$ of $\Gamma_1(N)$. Conjugation by A yields the matrices $\begin{pmatrix} 1-eg & e^2 \\ -g^2 & 1+eg \end{pmatrix}$, $\begin{pmatrix} 1+Nfh & -Nf^2 \\ Nh^2 & 1-Nfh \end{pmatrix}$, and $\begin{pmatrix} 1+N(eh+fg+fh-eg) & N(e^2-2ef-f^2) \\ N(h^2+2gh-g^2) & 1-N(eh+fg+fh-eg) \end{pmatrix}$ respectively. Now, the first (resp. second) conjugated element lies in $\Gamma_0(N)$ if and only if the first (resp. last) three asserted numbers are integral. Assuming this, we find by subtracting the corresponding multiples of these numbers that the third conjugated element is in $\Gamma_0(N)$ precisely when the remaining three numbers are in \mathbb{Z} . This proves the lemma. \square

We shall also make use of the following lemma.

Lemma 2.2. *Let α , β , π , ρ , κ , and N be integers, such that α and β are positive and $\gcd\{\alpha, \beta\}$, $\gcd\{\alpha, \rho\}$, and $\gcd\{\beta, \pi\}$ all equal 1. Assume that the quotients $\frac{\pi^2\alpha\kappa}{N\beta}$, $\frac{\rho^2\beta\kappa}{N\alpha}$, $\frac{\rho}{\alpha}\left(\frac{\kappa\pi\rho}{N}-1\right)$, $\frac{2\pi}{\beta}\left(\frac{\kappa\pi\rho}{N}-1\right)$, and $\frac{1}{\alpha\beta\kappa}\left(\frac{\kappa\pi\rho}{N}-1\right)^2$ are integers. Then $\alpha = \beta = 1$, and κ is a divisor of N .*

Proof. The integrality of the first two quotients, together with the co-primality conditions, imply that $\alpha\beta|\kappa$. Multiplying the third quotient by N , we find that

$\alpha|N$ as well. If N is even then multiplying the fourth quotient by $\frac{N}{2}$ yields the same assertion for β . If N is odd then $\beta|2N$, and we claim that β is odd. Indeed, multiplying the last quotient by N^2 renders a quotient whose numerator is odd if β is even, and β (and even β^2) appears in the denominator. Therefore $\alpha\beta|N$ as well. But then canceling $\alpha\beta$ from each expression involving $\frac{\kappa}{N}$ puts us back in the initial situation. Therefore $\alpha\beta$ divides both κ and N infinitely many times, so that it must equal 1. Substituting this and multiplying the last quotient by N , we find that κ divides $N + \frac{(\kappa\pi\rho)^2}{N}$. Let p be a prime, and assume that $v_p(\kappa) > v_p(N)$. But then $v_p(\frac{(\kappa\pi\rho)^2}{N}) > v_p(\kappa) > v_p(N)$, so that by adding N we obtain a number whose p -adic valuation equals precisely $v_p(N)$. But such a number cannot be divisible by κ if $v_p(\kappa) > v_p(N)$. This contradiction shows that $v_p(\kappa) \leq v_p(N)$ for every prime p , which amounts to κ dividing N . This proves the lemma. \square

We can now prove the desired assertion.

Proposition 2.3. *If conjugation by an element $A \in SL_2(\mathbb{R})$, written as in Lemma 2.1, sends $\Gamma_1(N)$ into $\Gamma_0(N)$, then $A \in \Gamma_0^{*,s_N}(N)$.*

Proof. Applying Lemma 2.1, we can use the integrality of the expressions appearing in that Lemma. If $g = 0$ then the fact that e^2 and h^2 are integers and $eh = 1$ (by the SL_2 condition) implies that $e = h = 1$. We have $f \in \frac{1}{N}\mathbb{Z}$ (since $Nfh \in \mathbb{Z}$), and the fact that Nf^2 is also integral implies that the denominator of the reduced form of $b = f$ must divide s_N . The assertion thus holds if $g = 0$, with $\mu = 1$.

We therefore assume that $g \neq 0$. Using the integrality of $\frac{g^2}{N} \in \mathbb{Z}$ from Lemma 2.1, and then of eg and $2gh$, we find that

$$g = \pm\sqrt{Nt} \quad \text{for some } t \in \mathbb{N}, \quad \text{as well as} \quad e = \frac{p}{\sqrt{Nt}} \quad \text{and} \quad h = \frac{q}{2\sqrt{Nt}} \quad (3)$$

with integers p and q . Since $h^2 \in \mathbb{Z}$ as well, we obtain $4Nt|q^2$, so that $2|q$ and we can write $h = \frac{r}{\sqrt{Nt}}$ with $r \in \mathbb{Z}$.

The analysis will be easier if we separate divisors. Let $\delta = \gcd\{t, p, r\} > 0$. Then the numbers $\alpha = \gcd\{\frac{t}{\delta}, \frac{p}{\delta}\}$ and $\beta = \gcd\{\frac{t}{\delta}, \frac{q}{\delta}\}$ are positive, co-prime, and both divide $\frac{t}{\delta}$. Hence the latter number is divisible by their product. We can thus write

$$p = \delta\alpha\pi, \quad r = \delta\beta\rho, \quad \text{and} \quad t = \delta\alpha\beta\tau, \quad \text{with} \quad \tau \in \mathbb{N}, \quad \pi \in \mathbb{Z}, \quad \text{and} \quad \rho \in \mathbb{Z},$$

satisfying the co-primality conditions

$$\gcd\{\tau, \pi\rho\} = 1, \quad \gcd\{\alpha, \beta\rho\} = 1, \quad \text{and} \quad \gcd\{\beta, \alpha\pi\} = 1. \quad (4)$$

Substituting these values of p , r , and t , as well as $f = \frac{eh-1}{g}$ from the SL_2 condition, transforms and extends Equation (3) to

$$e = \frac{\pi\sqrt{\delta\alpha}}{\sqrt{N\beta\tau}}, \quad g = \pm\sqrt{N\delta\alpha\beta\tau}, \quad h = \frac{\rho\sqrt{\delta\beta}}{\sqrt{N\alpha\tau}}, \quad \text{and} \quad f = \pm\frac{\frac{\delta\pi\rho}{N\tau} - 1}{\sqrt{N\delta\alpha\beta\tau}}, \quad (5)$$

where the two \pm signs are the same.

Now, the numerator of f must be integral (e.g., by the integrality of Nf^2 from Lemma 2.1), so that the first co-primality condition in Equation (4) implies that $\tau|\delta$. We therefore write $\delta = \kappa\tau$ with $\kappa \in \mathbb{N}$, and observing that the values of f and g in Equation (5) involve the expression $\pm\sqrt{\delta\tau} = \pm\sqrt{\kappa} \cdot \tau$, we can remove the assumption $\tau > 0$ and absorb the sign into τ . Now, the numbers from Lemma 2.2 are e^2 , h^2 , $Nfh\tau$, $2Nef\tau$, and $Nf^2\tau^2$, which are all integral by Lemma 2.1. Applying Lemma 2.2, we get $\alpha = \beta = 1$ and write N as $\kappa\nu$, and Equation (5) takes the form

$$e = \frac{\pi}{\sqrt{\nu}}, \quad g = \tau\kappa\sqrt{\nu}, \quad h = \frac{\rho}{\sqrt{\nu}}, \quad \text{and} \quad f = \frac{\frac{\pi\rho}{\nu} - 1}{\tau\kappa\sqrt{\nu}}. \quad (6)$$

We now use the integrality of e^2 and h^2 from Equation (6) to deduce that ν divides the square of $\gcd\{\pi, \rho\}$. Let J be the set of primes p dividing N which still divide $\frac{\gcd\{\pi, \rho\}^2}{\nu}$. The prime divisors of κ are not in J , since the integrality of $\kappa\nu b^2\tau^2$ from Lemma 2.1 (recall the decomposition of N) implies that κ divides the square of $\frac{\pi\rho}{\nu} - 1$, and the latter number is congruent to -1 modulo any prime lying in J . Therefore the divisor $\mu = \prod_{p \in J} p^{v_p(N)}$ divides ν , and the quotient is a square ω^2 since $v_p(\nu) = 2v_p(\gcd\{\pi, \rho\})$ for any prime divisor p of N not lying in J . The divisor μ is clearly exact, and by substituting $\nu = \omega^2\mu$ and $\kappa = \frac{N}{\omega^2\mu}$ in Equation (6) we find that A has the form from Definition 1.1 with the rational numbers $a = \frac{\pi}{\omega\mu}$, $c = \frac{\tau}{\omega}$, $d = \frac{\rho}{\omega\mu}$, and $b = \frac{\omega\mu}{N\tau}(\frac{\pi\rho}{\nu} - 1)$. The expressions involving squares which must be integral by Lemma 2.1 are $a^2\mu$, $d^2\mu$, $c^2\frac{N}{\mu}$, and $b^2\frac{N}{\mu}$, which shows that a , b , c , and d must satisfy the conditions from Definition 1.1. This completes the proof of the proposition. \square

The main technical tool for determining normalizers is the following refinement of Propositions 2.3 and 1.2.

Lemma 2.4. *Let H be a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$, take some $A \in \Gamma_0^{*,sN}(N)$, and present it as in Definition 1.1. Then A normalizes Γ_H if and only if the following conditions are satisfied:*

- (i) *The denominators of ab and cd divide any difference $e - h$ for an element $\gamma = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ in Γ_H .*
- (ii) *H contains the kernel of the projection onto $(\mathbb{Z}/K\mathbb{Z})^\times$, where $\frac{N}{K}$ is the least common multiple of the denominators of ac and bd .*
- (iii) *For any γ as in condition (i), changing the diagonal elements by $bc\frac{N}{\mu}(e - h)$ gives again an element of H .*

Remark 2.5. Condition (ii) in Lemma 2.4 is equivalent to H being invariant under additive translations by multiples of K . Indeed, the fact that $\frac{N}{K}|s_N$ shows that the primes dividing N already divide K , so that such translations

do not affect co-primality to N . As such a translation takes an element of $(\mathbb{Z}/N\mathbb{Z})^\times$ to its image under multiplication by an element of the kernel of the projection from that condition, this indeed proves the claim.

Proof. Consider the matrix from Equation (2), in which we assume that the matrix $\gamma = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ lies in Γ_H . Condition (i) is equivalent to the upper right entry there being integral, and to the lower left entry there being in $N\mathbb{Z}$. The interpretation of condition (ii) given in Remark 2.5 means, as the proof of Proposition 1.2 shows, that conjugation by A takes $\Gamma_1(N)$ into Γ_H . When these two conditions are satisfied, then the diagonal entries of the matrix from Equation (2) differ from that of A by $\pm bc\frac{N}{\mu}(e-h)$, up to expressions which are dealt with in condition (iii). Hence condition (iii) is equivalent, under the other two conditions, to normalizing Γ_H . This proves the lemma. \square

Using the groups $\Gamma_0^{*,\sigma}(N)$ from Definition 1.7, we can rephrase Lemma 2.4 in the following way.

Corollary 2.6. *If H is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ then we define K_H to be the minimal multiple of $s_N t_N$ such that the kernel of the projection from $(\mathbb{Z}/N\mathbb{Z})^\times$ to $(\mathbb{Z}/K_H\mathbb{Z})^\times$ is contained in H . We define $\sigma_H = \gcd\left\{\frac{N}{K_H}, \eta_H\right\}$, where η_H is the gcd of all the differences $e-h$ where e and h are integers which map to inverse elements of H . Then the normalizer of Γ_H is contained in $\Gamma_0^{*,\sigma_H}(N)$. More precisely, this normalizer consists of those elements $\begin{pmatrix} a\sqrt{\mu} & b/\sqrt{\mu} \\ c\frac{N}{\mu}\sqrt{\mu} & d\sqrt{\mu} \end{pmatrix}$ of $\Gamma_0^{*,\sigma_H}(N)$ such that if e and h are inverse elements of H then $ade\mu - bch\frac{N}{\mu}$ and $adh\mu - bce\frac{N}{\mu}$ are also inverse elements of H .*

Proof. We first observe that K_H is a well-defined divisor of N (since H contains the trivial subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$), and that for divisors K of N which are divisible by $s_N t_N$ the kernel of the map to $(\mathbb{Z}/K\mathbb{Z})^\times$ determines K . This is easily seen through the fact that $\frac{\varphi(N)}{\varphi(K)} = \frac{N}{K}$ for such divisors. Since we consider only elements of $\Gamma_0^{*,s_N}(N)$ (so that any σ is a divisor of s_N), condition (ii) of Lemma 2.4 is satisfied precisely for elements which lie in $\Gamma_0^{*,N/K_H}(N)$. It is now clear that $\eta_H|N$ (since $\begin{pmatrix} 1+N & 1 \\ N & 1 \end{pmatrix} \in \Gamma_1(N)$), and that condition (i) of Lemma 2.4 is satisfied for an element of $\Gamma_0^{*,N/K_H}(N)$ if and only if that element is in $\Gamma_0^{*,\sigma_H}(N)$. Now, the product of $ade\mu - bch\frac{N}{\mu}$ and $adh\mu - bce\frac{N}{\mu}$ is $eh - (e-h)^2 ad\mu \cdot bc\frac{N}{\mu}$, which is 1 plus a multiple of N plus a multiple of $N\frac{(e-h)^2}{\sigma_H^2}$ if $\begin{pmatrix} a\sqrt{\mu} & b/\sqrt{\mu} \\ c\frac{N}{\mu}\sqrt{\mu} & d\sqrt{\mu} \end{pmatrix} \in \Gamma_0^{*,\sigma_H}(N)$ by Remark 1.8. As $\sigma_H|e-h$, the asserted elements are indeed inverses. Now, as the terms which do not involve $ad\mu$ or $bc\frac{N}{\mu}$ in the diagonal entries in Equation (2) are multiples of $\frac{N}{\sigma_H}|K_H$ and H is invariant under such translations (see Remark 2.5), the latter assertion is equivalent to condition (iii) of Lemma 2.4. This proves the corollary. \square

Corollary 2.6 presents the maximal σ such that the normalizer of Γ_H is contained in $\Gamma_0^{*,\sigma}(N)$. In the other direction, we will be interested to know when

the smallest such group, namely the Atkin–Lehner group $\Gamma_0^*(N)$, is contained in that normalizer. For this we can prove the following result.

Proposition 2.7. (i) *The group $\Gamma_0^*(N)$ normalizes both $\Gamma_0(N)$ and $\Gamma_1(N)$. It operates on the quotient $(\mathbb{Z}/N\mathbb{Z})^\times$ via the quotient $\{\pm 1\}^{\{p|N\}}$, in an explicit way.*

(ii) *$\Gamma_0^*(N)$ normalizes Γ_H for a subgroup $H \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$ if and only if H is preserved under this action of $\{\pm 1\}^{\{p|N\}}$.*

Proof. The fact that $\Gamma_0^*(N)$ normalizes both groups follows easily from Lemma 2.4, or directly from the formula in Equation (2) (one can also observe that the kernel of the projection onto $\{\pm 1\}^{\{p|N\}}$ is precisely $\Gamma_0(N)$). As $\Gamma_0(N)/\Gamma_1(N)$ is Abelian, the action of $\Gamma_0^*(N)$ is via the quotient $\{\pm 1\}^{\{p|N\}}$. Equation (2) shows that elements of $\Gamma_0^*(N)$ which are associated to the exact divisor μ of N take an element $t \in (\mathbb{Z}/N\mathbb{Z})^\times$ to the element of $(\mathbb{Z}/N\mathbb{Z})^\times$ which is congruent to t modulo $\frac{N}{\mu}$, but whose residue modulo μ is the one which is inverse to t . This proves part (i), and part (ii) immediately follows from it. This proves the proposition. \square

Two types of natural subgroups of $(\mathbb{Z}/N\mathbb{Z})^\times$ which are of particular interest are the following ones. In case H is the kernel of the projection onto $(\mathbb{Z}/D\mathbb{Z})^\times$ for a divisor D of N , the group Γ_H is the intersection $\Gamma_0(N) \cap \Gamma_1(D)$, which we denote $\Gamma_{0,1}(N, D)$. In particular $\Gamma_{0,1}(N, 1) = \Gamma_0(N)$ and $\Gamma_{0,1}(N, N) = \Gamma_1(N)$. On the other hand, recall that the cardinality of $(\mathbb{Z}/N\mathbb{Z})^\times$ is given by *Euler’s totient function* $\varphi(N) = N \prod_{p|N} (1 - \frac{1}{p})$, while the exponent of that group is given by *Carmichael’s function* $\lambda(N)$. The value of the latter function is $\text{lcm}\{\lambda(p^{v_p(N)}) | p|N\}$, where on prime powers $p^{v_p(N)}$ Carmichael’s function λ coincides with φ , unless $p = 2$ and $v_2(N) \geq 3$ where it coincides with $\frac{\varphi}{2}$. Let m be a divisor of $\lambda(N)$, and take $H = (\mathbb{Z}/N\mathbb{Z})^\times[m]$ to be the subgroup consisting of those elements of $(\mathbb{Z}/N\mathbb{Z})^\times$ whose order divides m . We denote the associated group Γ_H by $\Gamma_1^{[m]}(N)$, so that $\Gamma_1^{[1]}(N)$ and $\Gamma_1^{[\lambda(N)]}(N)$ are just $\Gamma_1(N)$ and $\Gamma_0(N)$ respectively once more, and $\Gamma_1^{[2]}(N)$ is the group denoted $\Gamma_1^{\sqrt{1}}(N)$ in [LZ]. Proposition 2.7 therefore yields the following assertions:

Corollary 2.8. *$\Gamma_0^*(N)$ is contained in the normalizers of the following intermediate groups:*

- (i) $\Gamma_1^{[m]}(N)$ for any $m|\lambda(N)$.
- (ii) $\Gamma_{0,1}(N, D)$ for any $D|N$.
- (iii) Γ_H for any subgroup H of $(\mathbb{Z}/N\mathbb{Z})^\times[2]$.
- (iv) Any group which is generated by groups of the sort considered in parts (i), (ii), and (iii).

Proof. It suffices, by Proposition 2.7, to show that the corresponding groups are invariant under the action of $\{\pm 1\}^{\{p|N\}}$ described explicitly in the proof of Proposition. Part (i) thus follows from the fact that $(\mathbb{Z}/N\mathbb{Z})^\times[m]$ is a characteristic in $(\mathbb{Z}/N\mathbb{Z})^\times$ for any $m|\lambda(N)$. For part (ii) we consider $\{\pm 1\}^{\{p|D\}}$ as the quotient of $\{\pm 1\}^{\{p|N\}}$ as above, and observe that the action of the former group on $(\mathbb{Z}/D\mathbb{Z})^\times$ and of the latter group on $(\mathbb{Z}/N\mathbb{Z})^\times$ commute with the projection map from residues modulo N to residues modulo D . As this implies that the kernel of that projection is preserved under the action of $\{\pm 1\}^{\{p|N\}}$, the assertion of part (ii) follows. Part (iii) is easily established since the operation of $\{\pm 1\}^{\{p|N\}}$ is trivial on any element of $(\mathbb{Z}/N\mathbb{Z})^\times[2]$, and part (iv) is an immediate consequence of the previous ones. This proves the corollary. \square

Remark 2.9. Proposition 2.3 and Corollary 2.8 suffice to determine the normalizer of $\Gamma_1^{[m]}(N)$ for any divisor m of $\lambda(N)$, as well as of $\Gamma_{0,1}(N, D)$ for divisor D of N , as precisely $\Gamma_0^*(N)$ if N is square-free (this will also follow from the more general results of Theorems 3.1 and 3.8 below). On the other hand, there are examples of groups Γ_H whose normalizer does not contain $\Gamma_0^*(N)$, even in the square-free N case: Consider, for example, the case where $N = 91$ and H is the group generated by an element a whose images in both \mathbb{F}_7 and in \mathbb{F}_{13} generate the multiplicative groups of the corresponding field. Since a has order 12 in $(\mathbb{Z}/91\mathbb{Z})^\times$, any power of a is determined by its image in \mathbb{F}_{13}^\times . But the image of a under an element of $\Gamma_0^*(91)$ with $\mu = 7$ takes a to a residue which coincides with a modulo 13 but not modulo 7. Hence this image is not a power of a in $(\mathbb{Z}/91\mathbb{Z})^\times$, H is not preserved under $\{\pm 1\}^{\{p|N\}}$, and the normalizer of the associated congruence group of level 91 will be a proper subgroup of $\Gamma_0^*(91)$.

3 Normalizers of Congruence Subgroups

In this section we determine the normalizers of the several types of groups Γ_H , including the groups $\Gamma_{0,1}(N, D)$ with $D|N$ and $\Gamma_1^{[m]}(N)$ for $m|\lambda(N)$. We begin with the first family of congruence subgroups:

Theorem 3.1. *If D is a divisor of N then the normalizer of $\Gamma_{0,1}(N, D)$ is precisely $\Gamma_0^{*,\sigma}(N)$ for $\sigma = \gcd\{2D, \frac{N}{D}\} \cdot \frac{\gcd\{s_N, 24\}}{2^\theta \gcd\{s_N, 24, 2D\}}$, where θ equals 1 if $2v_2(D) = v_2(N) - 1$ and 0 otherwise.*

Proof. The group H is the kernel of the projection from $(\mathbb{Z}/N\mathbb{Z})^\times$ to $(\mathbb{Z}/D\mathbb{Z})^\times$. Before determining σ_H , we observe that the additional condition in Corollary 2.6 (i.e., condition (iii) of Lemma 2.4) is satisfied with this H by any element of $\Gamma_0^{*,s_N}(N)$, since $ad\mu$ and $bc\frac{N}{\mu}$ are integers with difference 1: Indeed, taking residues modulo D one may replace e and h by 1 and get the desired result. It follows that the normalizer of $\Gamma_{0,1}(N, D)$ is the full group $\Gamma_0^{*,\sigma_H}(N)$, and we need to show that $\sigma = \sigma_H$ has the asserted value. The number K_H from Corollary 2.6 is $\text{lcm}\{D, s_N t_N\}$, so that $\frac{N}{K_H}$ is $\gcd\{s_N, \frac{N}{D}\}$.

We claim that $\eta_H = \text{lcm}\{2D, \text{gcd}\{N, 24\}\}$, unless $\frac{N}{D}$ is odd, where $2D$ has to be replaced by D . The difference of any two inverses modulo N which are congruent to 1 modulo D is clearly divisible by D . We claim that if $\frac{N}{D}$ is even then it has to be divisible by $2D$. Indeed, if D is odd and N is even then all the diagonal entries of matrices in $\Gamma_{0,1}(N, D)$ are odd, hence congruent to 1 modulo $2D$. On the other hand, if both D and $\frac{N}{D}$ are even and $1 + kD$ and $1 + lD$ are inverses modulo N then $\frac{N}{D}$ divides $k + l + klD$, so that k and l must be of the same parity. Hence every such difference is divisible by D if $\frac{N}{D}$ is odd but by $2D$ if $\frac{N}{D}$ is even. But such a difference is also divisible by $\text{gcd}\{N, 24\}$ since $(\mathbb{Z}/24\mathbb{Z})^\times$ has exponent 2. Indeed, if $\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ is an element of $\Gamma_0(N)$ then e and h are residues which are inverse modulo $(N, 24)$, and therefore e and h coincide modulo $(N, 24)$ hence their difference is divisible by this number. As 24 is the maximal number K such that $(\mathbb{Z}/K\mathbb{Z})^\times$ has exponent 2, a simple argument using the Chinese Remainder Theorem and examining residues modulo 9 or 16 shows that no number larger than the asserted value divides all the differences $e - h$ for $\begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \Gamma_{0,1}(N, D)$. This determines η_H as the asserted number, so that σ_H is the gcd of $\frac{N}{D}$, s_N , and the value just determined of η_H . We may use $\text{lcm}\{2D, \text{gcd}\{N, 24\}\}$ for η_H in any case, since if $\frac{N}{D}$ is odd then either s_N is odd or $v_2(D) > v_2(s_N)$, so that this value yields the correct gcd with s_N (hence the correct σ_H) in any case.

It remains to show that this gcd yields the asserted value. Replacing η_H by simply $2D$ would give just the first multiplier divided by 2^θ , since $v_p(2D)$ and $v_p(\frac{N}{D})$ cannot both exceed $v_p(s_N)$ for any prime p , unless $p = 2$ and the equality yielding $\theta = 1$ holds. Now, if $v_p(2D) \geq v_p(s_N)$ for some prime p then the powers of p dividing $\text{gcd}\{s_N, \eta_H\}$ and $\text{gcd}\{s_N, 2D\}$ are both $p^{v_p(s_N)}$, while if $v_p(2D) \geq v_p(24)$ (this is always the case for $p > 3$) then $v_p(\eta_H) = v_p(2D)$ and again $\text{gcd}\{s_N, \eta_H\}$ and $\text{gcd}\{s_N, 2D\}$ are divisible by the same power of p . But those are, by definition, the primes p which do not divide the quotient $\frac{\text{gcd}\{s_N, 24\}}{\text{gcd}\{s_N, 24, 2D\}}$. On the other hand, if $v_p(2D) < \min\{v_p(s_N), v_p(24)\}$ then the power of p which divides that quotient is the difference between the latter two expressions. But in this case we have $v_p(\frac{N}{D}) > v_p(s_N) > v_p(2D)$ and $v_p(\eta_H) = v_p(24)$, so that we compare $v_p(\sigma_H) = \min\{v_p(s_N), v_p(24)\}$ with $v_p(2D)$ again. Therefore $\sigma_H = \text{gcd}\{\frac{N}{D}, s_N, \eta_H\}$ equals the asserted value (since both are positive numbers which are divisible by the same prime powers), which completes the proof of the theorem. \square

We therefore recover the results of [CN], [AL], [AS], [B], and others about the normalizers of the classical congruence groups:

Corollary 3.2. *The normalizer of $\Gamma_1(N)$ is $\Gamma_0^*(N)$. The normalizer of $\Gamma_0(N)$ is $\Gamma_0^{*, \text{gcd}\{s_N, 24\}}(N)$.*

Proof. For $\Gamma_1(N)$ we take $D = N$ in Theorem 3.1. Then $\frac{N}{D} = 1$ and $\text{gcd}\{s_N, 24\}$ divides $2D$, so that $\sigma = 1$ and the normalizer is $\Gamma_0^*(N)$. On the other hand, the result for $\Gamma_0(N)$ is obtained by taking $D = 1$ in Theorem 3.1, which yields the value $\frac{\text{gcd}\{2, N\} \text{gcd}\{s_N, 24\}}{2^\theta \text{gcd}\{s_N, 2\}}$ for σ . We have to show that this expression reduces to

$\gcd\{s_N, 24\}$, i.e., the combination of the other three multipliers cancel to 1. But if N is odd then all the multipliers are 1, if $v_2(N) = 1$ then $2^\theta = 2$ and s_N is odd, and if $4|N$ then $2|s_N$ but $\theta = 0$ once more. This proves the corollary. \square

The discrepancy between our Corollary 3.2 and the main result of [L1] in case $N = 4$ arises from the fact that this reference considers subgroups of $PSL_2(\mathbb{Z})$. The group we must consider in this case is the one generated by $\Gamma_1(N)$ and $\{\pm I\}$. The result of [L1] is thus recovered as a special case of the following proposition.

Proposition 3.3. *Let N and D be as in Theorem 3.1. Then the normalizer of $\pm\Gamma_{0,1}(N, D)$ coincides with that of $\Gamma_{0,1}(N, D)$, unless $N = D = 4$ where it coincides with that of $\Gamma_0(4)$.*

Proof. Our group H is the product of the image of ± 1 in $(\mathbb{Z}/N\mathbb{Z})^\times$ with the kernel of the projection to $(\mathbb{Z}/D\mathbb{Z})^\times$. Parts (ii), (iii), and (iv) of Proposition 2.8 show that the normalizer must contain $\Gamma_0^*(N)$. On the other hand, the number η_H , which is based on divisibility of differences between inverse elements of H , is not affected by multiplication by -1 . In addition, K_H is based on the intersection of H with the image of $1 + s_N t_N \mathbb{Z}$ modulo N , and -1 is not there unless $s_N t_N$ is 1 or 2, i.e., unless N is a divisor of 4. Moreover, the only case where $N|4$ and $-I \notin \Gamma_{0,1}(N, D)$ is where $N = D = 4$. This shows that the normalizer of $\pm\Gamma_{0,1}(N, D)$ is contained in the one of $\Gamma_{0,1}(N, D)$ unless $N = D = 4$, and the reverse inclusion follows immediately from the centrality of $-I$ in $SL_2(\mathbb{R})$. As for $N = D = 4$ we get $\pm\Gamma_{0,1}(N, D) = \Gamma_0(4)$, this completes the proof of the proposition. \square

The assertion from [L1] is just the following corollary.

Corollary 3.4. *The normalizer of $\pm\Gamma_1(N)$ is $\Gamma_0^*(N)$ if $N \neq 4$, and it is $\Gamma_0^{*,2}(4)$ in case $N = 4$. The latter group contains $\Gamma_0^*(N)$ as a subgroup of index 3.*

Proof. This is just the case $D = N$ in Proposition 3.3. The assertion thus follows from Corollary 3.2, and the index is obtained by comparing the indices of $\Gamma_0(4)$ in the two groups, which are evaluated in Proposition 1.9. This proves the corollary. \square

In Theorem 3.1 we consider congruences only on three of the entries of the matrices. But a simple argument allows us to extend the result to more general congruence subgroups.

Theorem 3.5. *Let T , M , and D be positive integers such that $D|N = MT$, and define σ to be as in Theorem 3.1 (with $N = MT$).*

- (i) *The set Γ of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ in which $T|c$, $M|b$, and a and d are congruent to 1 modulo D is a subgroup of $SL_2(\mathbb{Z})$.*

- (ii) The normalizer of Γ in $SL_2(\mathbb{R})$ consists of all those matrices having a presentation as $\begin{pmatrix} a\sqrt{\mu} & b\frac{M}{\mu}\sqrt{\mu} \\ c\frac{\pi}{\mu}\sqrt{\mu} & d\sqrt{\mu} \end{pmatrix}$ in which μ is an exact divisor of N and a, b, c , and d are rational numbers such that multiplying a or d by $\gcd\{\sigma, s_\mu\}$ and multiplying b or c by $\gcd\{\sigma, s_{N/\mu}\}$ yield integers.
- (iii) Γ has index $D\sigma^2 \prod_{p|D} (1 - \frac{1}{p}) \prod_{p|\sigma, v_p(N)=2v_p(\sigma)} (1 + \frac{1}{p}) \cdot \prod_{p|N/\sigma^2} 2$ in its normalizer.

Proof. Part (i) follows either from direct evaluation of products and inverses of elements of Γ , or from observing that conjugation by $\frac{1}{\sqrt{M}} \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$ takes the subgroup $\Gamma_{0,1}(N, D)$ directly onto Γ . The latter argument shows that the normalizer of Γ is the image of that of $\Gamma_{0,1}(N, D)$ under conjugation by the same element. As the latter normalizer is determined in Theorem 3.1 as $\Gamma_0^{*,\sigma}(N)$, part (ii) also follows from that conjugation, using Definition 1.7. For part (iii) it suffices to determine the index of $\Gamma_{0,1}(N, D)$ in its normalizer. Now, part (iii) of Proposition 1.9 shows that the index of $\Gamma_0(N)$ in $\Gamma_0^{*,\sigma}(N)$ is $\sigma^2 \prod_{p|\sigma, v_p(N)=2v_p(\sigma)} (1 + \frac{1}{p}) \cdot \prod_{p|N/\sigma^2} 2$. As the index of $\Gamma_{0,1}(N, D)$ in $\Gamma_0(N)$ is $\varphi(D) = D \prod_{p|D} (1 - \frac{1}{p})$ (since H is the kernel of a surjective homomorphism onto $(\mathbb{Z}/D\mathbb{Z})^\times$), part (iii) is also established. This proves the theorem. \square

The normalizers of the various congruence subgroups defined at the beginning of Section 1 all follow as corollaries, including the classical result about the normalizers of the principal congruence subgroups.

Corollary 3.6. *Let N and M be integers.*

- (i) The normalizer of $\Gamma^1(M)$ consists of matrices of the form $\begin{pmatrix} a\sqrt{\mu} & b\frac{M}{\mu}\sqrt{\mu}\sqrt{\mu} \\ c/\sqrt{\mu} & d\sqrt{\mu} \end{pmatrix}$ in which μ is an exact divisor of M and a, b, c , and d are integers.
- (ii) The normalizer of $\Gamma^0(M)$ includes precisely the matrices $\begin{pmatrix} a\sqrt{\mu} & b\frac{M}{\mu}\sqrt{\mu}\sqrt{\mu} \\ c/\sqrt{\mu} & d\sqrt{\mu} \end{pmatrix}$ with μ an exact divisor of M , and here a, b, c , and d satisfy the conditions for the corresponding coordinates of $\Gamma_0^{*,\gcd\{s_M, 24\}}(N)$.
- (iii) More generally, if $D|M = N$ and σ is as in Theorem 3.1 then the normalizer of $\Gamma^{0,1}(N, D) = \Gamma^0(N) \cap \Gamma^1(D)$ is the set of matrices $\begin{pmatrix} a\sqrt{\mu} & b\frac{N}{\mu}\sqrt{\mu}\sqrt{\mu} \\ c/\sqrt{\mu} & d\sqrt{\mu} \end{pmatrix}$ such that $\begin{pmatrix} a\sqrt{\mu} & b/\sqrt{\mu} \\ c\frac{N}{\mu}\sqrt{\mu} & d\sqrt{\mu} \end{pmatrix} \in \Gamma_0^{*,\sigma}$.
- (iv) The normalizer of $\Gamma_0^0(T, M)$ is obtained by taking the matrices of the form $\begin{pmatrix} a\sqrt{\mu} & b\frac{M}{\mu}\sqrt{\mu} \\ c\frac{\pi}{\mu}\sqrt{\mu} & d\sqrt{\mu} \end{pmatrix}$ where μ, a, b, c , and d are as in Definition 1.7 for $\Gamma_0^{*,\gcd\{s_N, 24\}}(N)$, with $N = MT$.
- (v) The normalizer of $\Gamma_1^0(T, M)$ (resp. $\Gamma_0^1(T, M)$) consists of all those matrices $\begin{pmatrix} a\sqrt{\mu} & b\frac{M}{\mu}\sqrt{\mu} \\ c\frac{\pi}{\mu}\sqrt{\mu} & d\sqrt{\mu} \end{pmatrix}$, with μ an exact divisor of $N = MT$ and where a, b, c , and

d are as in the definition of $\Gamma_0^{*,\sigma}(N)$, where σ is $\frac{\gcd\{2T,M\}\gcd\{s_N,24\}}{\gcd\{s_N,24,2T\}}$ if $v_2(2T) \neq v_2(M)$ and half of that value in case $v_2(2T) = v_2(M)$ (resp. $\frac{\gcd\{2M,T\}\gcd\{s_N,24\}}{\gcd\{s_N,24,2M\}}$, but divided by 2 if $v_2(2M) = v_2(T)$).

(vi) The normalizer of $\Gamma(M)$ is precisely $SL_2(\mathbb{Z})$.

Proof. Parts (iv) and (v) follow from Theorem 3.5 by taking D to be 1, T , or M . For part (vi) we take $M = T$ in part (v), and as $s_{M^2} = M$ and $v_2(2M) \neq v_2(M)$ we find that $\sigma = M$ as well. The desired assertion now follows from the fact that the conditions on a , b , c , and d are satisfied (regardless of μ —see Corollary 1.3 or part (ii) of Proposition 1.9 imply in this case) precisely when the entries of the matrices in the normalizer are integral. For part (iii) we substitute $T = 1$ in Theorem 3.5, and the result is analogous to Theorem 3.1. Parts (i) and (ii) follow from part (iii) in the same way as Corollary 3.2 follows from Theorem 3.1. This proves the corollary. \square

We now turn to subgroups defined by their exponents.

Lemma 3.7. *Let N be an integer, let p be a prime divisor of N , let m be a divisor of $\lambda(N)$, and take $H = (\mathbb{Z}/N\mathbb{Z})^\times[m]$.*

- (i) *The number K_H from Corollary 2.6 equals $\frac{N}{\gcd\{m, s_N\}}$.*
- (ii) *If p is a prime divisor of N and $\gcd\{p-1, m\} > 2$ then p does not divide the number η_H from Corollary 2.6.*
- (iii) *In case $\gcd\{p-1, m\}$ is 1 or 2 and p is odd, the power of p which divides η_H is $\max\{1, v_p(N) - v_p(m)\}$.*
- (iv) *The power $v_2(\eta_H)$ equals $\max\{3, v_2(N) - v_2(m) + 1\}$ when $8|N$ and m is even, and just $v_2(N)$ otherwise.*

Proof. The kernel of the projection from $(\mathbb{Z}/N\mathbb{Z})^\times$ to $(\mathbb{Z}/s_N t_N \mathbb{Z})^\times$, namely $(1 + s_N t_N \mathbb{Z})/N\mathbb{Z}$, is isomorphic to the cyclic group $s_N t_N \mathbb{Z}/N\mathbb{Z}$, of order s_N . Indeed, since $N|(s_N t_N)^2$ we find that the product of $1 + k s_N t_N$ with $1 + l s_N t_N$ equals $1 + (k+l) s_N t_N$ modulo N . In fact, $s_N t_N$ is the smallest divisor of N with that property. Hence its m -torsion part is its torsion part of order $\gcd\{m, s_N\}$, which is generated by the image of $1 + \frac{N}{\gcd\{m, s_N\}}$ modulo N . This proves part (i).

We now recall from the Chinese Remainder Theorem that $(\mathbb{Z}/N\mathbb{Z})^\times$ decomposes as the product $\prod_{p|N} (\mathbb{Z}/p^{v_p(N)}\mathbb{Z})^\times$. Moreover, the components for odd primes p are cyclic, while if $8|N$ then the component corresponding to $p = 2$ is the product of $\{\pm 1\}$ and a cyclic group (if $v_2(N) \leq 2$ then this component is also cyclic, of order 1 or 2). This decomposition clearly goes over to a similar decomposition of $H = (\mathbb{Z}/N\mathbb{Z})^\times[m]$ as $\prod_{p|N} (\mathbb{Z}/p^{v_p(N)}\mathbb{Z})^\times [\gcd\{m, \lambda(p^{v_p(N)}\mathbb{Z})\}]$. Now, the condition from part (ii) occurs only for odd $p \geq 5$, and it implies that

the image modulo p of any generator of $(\mathbb{Z}/p^{v_p(N)}\mathbb{Z})^\times [\gcd\{m, \lambda(p^{v_p(N)}\mathbb{Z})\}]$, which must have order $\gcd\{p-1, m\}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, differs from its inverse modulo p . As this element e and its inverse h provide us a difference $e - h$ which is not divisible by p , part (ii) follows.

On the other hand, if $\gcd\{p-1, m\}$ is 1 or 2 then the order of torsion inside $(\mathbb{Z}/p^{v_p(N)}\mathbb{Z})^\times$ in which we are interested is $p^{\min\{v_p(N)-1, v_p(m)\}}$ (perhaps multiplied by 2), except when $p = 2$ and $v_2(N) \geq 3$, where $\lambda(p^{v_p(N)}) = \varphi(p^{v_p(N)})$ and the -1 has to be replaced by -2 . Now, if p is odd then elements of torsion order p^r (resp. $2p^r$) for $r < v_p(N)$ inside $(\mathbb{Z}/p^{v_p(N)}\mathbb{Z})^\times$ are the images of $1 + p^{v_p(N)-r}\mathbb{Z}$ (resp. $\pm 1 + p^{v_p(N)-r}\mathbb{Z}$) modulo $p^{v_p(N)}$, and the inverse of an element of the form $\pm 1 + ap^{v_p(N)-r}$ modulo $p^{v_p(N)}$ is congruent to $\pm 1 - ap^{v_p(N)-r}$ modulo $p^{v_p(N)-r+1}$. As this shows that their difference is divisible precisely by $p^{v_p(N)-r}$ if a is not divisible by p , part (iii) is also established by substituting $r = \min\{v_p(N) - 1, v_p(m)\}$. For powers of 2 we note that if $8|N$ then the elements of order 2^r with $0 < r < v_2(N)$ arise from $\pm 1 + 2^{v_2(N)-r}\mathbb{Z}$, and the fact that the inverse of $\pm 1 + a \cdot 2^{v_2(N)-r}$ with odd a is $\pm 1 - a \cdot 2^{v_2(N)-r}$ modulo $2^{v_2(N)-r+2}$ implies that the power of 2 which divides the corresponding difference is $v_2(N) - r + 1$. This yields the assertion of part (iv) (since r is $\min\{v_2(N) - 2, v_2(m)\}$ here), since the cases where m is odd or where $v_2(N) \leq 2$ are trivial. This proves the lemma. \square

We can now prove our result about these types of groups.

Theorem 3.8. *For N and m as in Lemma 3.7, we define σ to be the number*

$$\prod_{\substack{p \mid \gcd\{m, s_N\} \\ \gcd\{p-1, m\} \leq 2}} p^{\max\{1, \min\{v_p(m), v_p(2N)-v_p(m)\}\}} \cdot 2^{\varepsilon - \max\{\theta, v_2(s_N)\}},$$

where θ is 1 if $2v_2(m) = v_2(N) + 1$ and 0 otherwise (as in Theorem 3.1), and ε equals 2 if $v_2(m) \geq v_2(N) \geq 6$, 1 if $v_2(m) = v_2(N) - 1 \geq 5$ or if $v_2(m) = v_2(N) \in \{4, 5\}$, and 0 otherwise. Then the normalizer of $\Gamma_1^{[m]}(N)$ is precisely $\Gamma_0^{*, \sigma}(N)$.

Proof. First we prove that the number σ_H from Corollary 2.6 is the asserted one. That Corollary evaluates it as the gcd of the two numbers $\frac{N}{K_H}$ and η_H , both of which are evaluated explicitly in Lemma 3.7. Clearly only primes p which divide $\gcd\{m, s_N\}$, which equals $\frac{N}{K_H}$ by part (i) of Lemma 3.7, can divide σ_H , and the condition $\gcd\{p-1, m\} \leq 2$ is also imposed since part (ii) of Lemma 3.7 shows that primes not satisfying it do not divide η_H . Now, if p is an odd prime such that $\gcd\{p-1, m\} \leq 2$ then we deduce from parts (i) and (iii) of Lemma 3.7 that $v_p(\sigma_H)$ is the minimum of $v_p(m)$, $v_p(s_N)$, and $\max\{1, v_p(N) - v_p(m)\}$, all of which are at least 1. We may omit $v_p(s_N)$ since either $v_p(m)$ or $v_p(N) - v_p(m)$ do not exceed it (and the inequality $v_p(s_N) \geq 1$ is obvious), and it is easy to see that for $v_p(m) > 0$ the minimum of the remaining two numbers is $\max\{1, \min\{v_p(m), v_p(2N) - v_p(m)\}\}$, where the extra multiplier of 2 does not affect the value of v_p since p is odd.

We still need to determine the power of 2 which divides σ_H , in case both m and s_N are even (the gcd condition is always satisfied). Parts (i) and (iv) of Lemma 3.7 determine it as the minimum of Corollary 2.6 $v_2(m)$, $v_2(s_N)$, and $\max\{3, v_2(2N) - v_2(m)\}$, unless $v_2(N) = 2$ (it cannot be smaller if $2|s_N$) and the third number is 2. We have to show that this minimum coincides with $\max\{1, \min\{v_2(m), v_2(2N) - v_2(m)\}\} - \theta$ up to the asserted discrepancy ε (the exponent of 2 includes $\max\{v_2(s_N), \theta\}$ rather than just θ in order to exclude the case with $v_2(N) = v_2(m) = 1$, where $\theta = 1$ and 2 does not divide s_N). In the case where $v_2(m) \leq v_2(N) - 2$ (so that taking the maximum with 3 does not change $v_2(2N) - v_2(m)$), the proof of Theorem 3.1 shows that there is no discrepancy. The case where $v_2(s_N) = 1$ also yields discrepancy 0, since both final numbers equal 1. Now, if $v_2(m) = v_2(N) - 1 \geq 3$ then we have to compare $\min\{3, v_2(s_N)\}$ with 2, which corresponds with ε being 1 if $v_2(N) \geq 6$ but 0 when $v_2(s_N) = 2$. Finally, if $v_2(m) \geq v_2(N)$ then we have the discrepancy between $\min\{3, v_2(s_N)\}$ and 1, which equals 2 in case $v_2(N) \geq 6$ and 1 if $v_2(s_N) = 2$. This completes the determination of σ_H as the asserted value.

It remains to consider the condition from Corollary 2.6. But the proof of Lemma 3.7 shows that when we consider residues modulo $p^{v_p(N)}$, one of two situations may occur: Either p does not divide σ_H , or the residues of the entries e and h lie in H if and only if they are congruent to 1 (or to ± 1) modulo p^r for some fixed power r . In the first case the numbers $ade\mu - bch\frac{N}{\mu}$ and $adh\mu - bce\frac{N}{\mu}$ are either e and h or h and e modulo $p^{v_p(N)}$ (depending on whether p divides $\frac{N}{\mu}$ or μ), while in the second case we take the residue modulo p^r and obtain that our numbers are congruent to e and to h modulo p^r as well. As both operations preserve the m -torsion modulo $p^{v_p(N)}$ (as in the proof of Theorem 3.1 and Proposition 3.3), hence also modulo N by the Chinese Remainder Theorem, we deduce from Corollary 2.6 that the full group $\Gamma_0^{*,\sigma}(N)$ normalizes $\Gamma_1^{[m]}(N)$. This proves the theorem. \square

Remark 3.9. The appearance of the maximum (with 1 or 3) in Lemma 3.7 and Theorem 3.8 is not redundant. There exist cases where some prime p may divide $2N$ (and even s_N), but can divide m to a larger power. To give examples, consider $N = 68$, with $v_2(N) = 2$ but whose λ -value 16 has $v_2 = 4$, or $N = 9 \cdot 163$, where $v_3(N) = 2$ but the divisor $163 - 1$ of $\lambda(N)$ is divisible by 3^4 .

The special case of prime m in Theorem 3.8 is of particular interest.

Corollary 3.10. *If N is a number such that $\lambda(N)$ is divisible by a prime number l then the normalizer of $\Gamma_1^{[l]}(N)$ is $\Gamma_0^{*,l}(N)$ if $l|s_N$ and just $\Gamma_0^*(N)$ otherwise.*

Proof. The only prime we must consider in Theorem 3.8 is $p = l$, and only in the case $l|s_N$. The gcd condition is immediate, and it is clear that the power is $v_l(l) = 1$ (also when $l = 2$, since $\theta = 0$ if $2|s_N$ and we are in the situation where $v_2(m) < 5$, hence $\varepsilon = 0$). The assertion thus follows from Theorem 3.8. This proves the corollary. \square

Our results can now be used to determine the normalizer of Γ_H for any subgroup H of $(\mathbb{Z}/N\mathbb{Z})^\times$ in case N is a prime power.

Proposition 3.11. *Let l be a prime, and take $N = l^u$ for some integer u .*

- (i) *If l is odd then any group between $\Gamma_1(N)$ and $\Gamma_0(N)$ is of the form $\Gamma_1^{[m]}(N)$ for some divisor m of $\lambda(N) = \varphi(N) = (l-1)l^{u-1}$, which is of the form kl^w for some $k|l-1$ and $0 \leq w < u$. The corresponding normalizer is $\Gamma_0^*(N)$ if $k > 2$ and is $\Gamma_0^{*,\sigma}(N)$ for $\sigma = l^{\min\{w, u-w\}}$ if $k \leq 2$.*
- (ii) *If $l = 2$ then any group between $\pm\Gamma_1(N)$ and $\Gamma_0(N)$ can be considered as $\Gamma_1^{[m]}(N)$ for $m = 2^w$ with $w \leq u-2$, where if $8|N$ then $\pm\Gamma_1(N)$ itself is associated with $m = 1$ (even though it does not equal $\Gamma_1^{[1]}(N) = \Gamma_1(N)$). When $u \leq 2$ then we take $m = u-1$. The normalizer then equals $\Gamma_0^{*,\sigma}(N)$, with σ being $2^{\min\{w, u+1-w\}-\theta}$ where θ is 1 if $2w = u+1$ and 0 otherwise.*
- (iii) *In case $l = 2$, $u \geq 2$, and the group H contains only elements which are congruent to 1 modulo 4 then our group is of the form $\Gamma_{0,1}(N, D)$ for some $D = 2^{u-w}$ with $w \leq u-2$. In this case the normalizer is $\Gamma_0^{*,\sigma}(N)$ for $\sigma = 2^{\min\{w, u+1-w\}-\theta}$ with θ as in part (ii).*
- (iv) *The remaining case is where $u \geq 3$ and the group is generated by some element which is congruent to -1 modulo 4. Such a group intersects the image of $1+s_N t_N \mathbb{Z}$ in the kernel of the projection to $(\mathbb{Z}/2^{u-w}\mathbb{Z})^\times$ for some $0 \leq w \leq u-3$, and the normalizer is $\Gamma_0^{*,\sigma}(N)$ where σ is just $2^{\min\{w, u-w\}}$.*

Proof. The first assertion in part (i) follows from the cyclicity of $(\mathbb{Z}/N\mathbb{Z})^\times$ for N an odd prime power. Examining the group described in Theorem 3.8, we find that the only prime which may divide s_N is $p = l$, and the corresponding gcd is k . The assertion is thus established in case $k > 2$, and if $k \leq 2$ we see that the difference $v_p(N) - v_p(m) = u - w$ is at least 1, so that the minimum is ≥ 1 if $l|m$ and 0 otherwise (the case $k = 1$ can also be established by taking $D = p^{u-w} > 1$ in Theorem 3.1, since the quotient appearing in that Theorem is trivial wherever D and N are non-trivial powers of the same odd prime). This establishes part (i) since $v_l(2N) = u$ for odd l . For the remaining parts we recall the structure of $(\mathbb{Z}/N\mathbb{Z})^\times$ for $N = 2^u$ with $u \geq 2$ (if $u = 1$ then this group is trivial) as $\{\pm 1\}$ times the cyclic group of the residues which are congruent to 1 modulo 4. This proves the first assertions in all three parts, so that part (iii) now follows from Theorem 3.1 since the quotient appearing there is trivial for s_N a power of 2 and D divisible by 4. Part (ii) is now a consequence of Theorem 3.8 since $\varepsilon = 0$ for $1 \leq v_2(m) \leq v_2(N) - 2$ there, complemented by the case where H is just the image of $\{\pm 1\}$ to which we associated the value $m = 1$ for $N \neq 4$ and $m = 2$ for $N = 4$, proved in Corollary 3.4. In part (iv) we recall that our group contains, apart from the kernel of the projection to $(\mathbb{Z}/2^{u-w}\mathbb{Z})^\times$, also elements which are to -1 precisely modulo 2^{u-1-w} . The same argument from the proof of Theorem 3.1 shows that the normalizer is $\Gamma_0^{*,\sigma}(N)$ where σ is 2 raised to the power which is the minimum of w , $v_2(s_N)$, and $\max\{3, u-w\}$.

(since we use $D = 2^{u-w}$ for finding K_H but $D = 2^{u-1-w}$ for determining η_H). One then deduces that $\sigma = 2^{\min\{w, u-w\}}$, since $u - w \geq 3$ and $v_2(s_N)$ is not smaller than either w or $u - w$. This proves the proposition. \square

The groups considered in Theorems 3.1 and 3.8 can be combined to yield, e.g., groups of elements of $(\mathbb{Z}/N\mathbb{Z})^\times$ whose m th power is trivial modulo D . We shall not carry out the examination of these groups in general, but just mention that in the case $m = 2$, which is related to lattices by Theorem 4.2 below, we have $D|\eta_H$ and $K_H = \text{lcm}\{s_N t_N, \frac{D}{\gcd\{2, D\}}\}$ (the denominator making sure that only integers are considered). Hence σ_H is divisible by $\sigma = \gcd\{D, \frac{2N}{D}\}/2^\theta$, with θ being 1 if $2v_2(D) = v_2(N)+1$ and 0 otherwise (and it probably equals that number, except perhaps for a few small values of $v_2(D)$), and one easily verifies that $\Gamma_0^{*,\sigma}(N)$ is contained in the normalizer in question. Indeed, Theorem 4.2 below shows that the corresponding group Γ_H will be the discriminant kernel of a lattice $L(N, D)$, whose group of automorphisms (arising from $SL_2(\mathbb{R})$) is $\Gamma_0^{*,\sigma}(N)$. The general case, as well as the fine details of this case, is left for future investigation.

4 Lattices

Consider the space $M_2(\mathbb{R})_0$ of traceless 2×2 real matrices. With the bilinear form $(X, Y) = \text{Tr}(XY)$ (so that $(X, X) = -2 \det X$) it becomes a real quadratic space of signature $(2, 1)$. The space $M_2(\mathbb{R})_0$ has a convenient basis, consisting of the three matrices

$$E = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \text{and} \quad F = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

E and F span a hyperbolic plane, and H is orthogonal to both of them and pairs to 2 with itself.

The connected component $SO^+(M_2(\mathbb{R})_0)$ of the orthogonal group of this vector space is isomorphic to $PSL_2(\mathbb{R})$, as one sees by letting $SL_2(\mathbb{R})$ act on $M_2(\mathbb{R})_0$ by conjugation. The action of an element $A = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in SL_2(\mathbb{R})$, whose inverse $A^{-1} = \begin{pmatrix} h & -f \\ -g & e \end{pmatrix}$, sends our basis elements to

$$\begin{pmatrix} -eg & e^2 \\ -g^2 & eg \end{pmatrix}, \quad \begin{pmatrix} eh + fg & -2ef \\ 2gh & -eh - fg \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} fh & -f^2 \\ h^2 & -fh \end{pmatrix} \quad (7)$$

respectively. Hence using the basis $-E$, $\frac{1}{2}H$, and F we get the natural formula for the action of the symmetric square representation.

Let $N \in \mathbb{N}$ and a divisor D of N be given. We define $L(N, D)$ to be the lattice spanned by $\frac{\sqrt{D}}{\sqrt{N}}E$, $\sqrt{ND} \cdot F$, and $\frac{\sqrt{N}}{\sqrt{D}}H$. It is isomorphic to the orthogonal direct sum of a hyperbolic plane rescaled by D and a 1-dimensional lattice generated by a vector of norm $\frac{2N}{D}$. The lattice $L_0(N) = L(N, 1)$ is the one considered in [BO], while [LZ] considers the lattice $L(N, N)$, which is denoted there $L_1(N)$.

The dual lattice $L^*(N, D) = \text{Hom}(L(N, D), \mathbb{Z})$ is identified as a subgroup of $M_2(\mathbb{R})_0$ via the bilinear form, and it is generated by $\frac{1}{\sqrt{DN}}E$, $\frac{\sqrt{N}}{\sqrt{D}}F$, and $\frac{\sqrt{D}}{2\sqrt{N}}H$. We wish to determine pre-image of the group $SAut^+(L(N, D))$ (the group of automorphisms of $L(N, D)$ which lie in the connected component $SO^+(M_2(\mathbb{R})_0)$), as well as its *discriminant kernel*, i.e., the subgroup of $SAut^+(L(N, D))$ which operates trivially on the discriminant group $L^*(N, D)/L(N, D)$.

The determination of the pre-image of $SAut^+(L(N, D))$ begins with the following observation.

Lemma 4.1. *Any matrix in $SL_2(\mathbb{Z})$ whose action preserves $L(N, D)$ must lie in $\Gamma_0^{*, s_N}(N)$.*

Proof. We know that rescaling of a lattice, i.e., multiplication of all of its generators by the square root of some integer, leaves the group $SAut^+(L(N, D))$ invariant. We therefore rescale $L(N, D)$ by $\frac{N}{D}$, and obtain the lattice generated by E , NF , and $\frac{N}{D}H$. All of these lattices are contained in $L_1(N)$ (with generators E , NF , and H), and contain the rescaling $\tilde{L}_0(N)$ of $L_0(N)$ by N (generators of which can be taken to be E , NF , and NH). It follows that if the action of the matrix $A = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in SL_2(\mathbb{R})$ preserves $L(N, D)$ then it must take $\tilde{L}_0(N)$ into $L_1(N)$. But the operation of A sends the basis of $\tilde{L}_0(N)$ to the matrices given in Equation (7), with the middle and right matrices multiplied by N . The resulting matrices lie in $L_1(N)$ if and only if the expressions e^2 , eg , $\frac{g^2}{N}$, $2Nef$, $N(eh + fg)$, $2gh$, Nf^2 , Nfh , and h^2 , which represent these matrices in terms of the basis for $L_1(N)$, all being integral. As these numbers are precisely the ones appearing in Lemma 2.1, we deduce from Proposition 2.3 that A must be in $\Gamma_0^{*, s_N}(N)$. This proves the lemma. \square

We can now prove our main result concerning automorphisms lattices. We shall allow ourselves the abuse of notation denoting $SAut^+(L(N, D))$ also the subgroup of $SL_2(\mathbb{R})$ which lies over the automorphism group (which is a subgroup of $PSL_2(\mathbb{R})$ by definition). The same applies for its subgroups, in particular the discriminant kernel.

Theorem 4.2. (i) $SAut^+(L(N, D))$ is the group $\Gamma_0^{*, \sigma}(N)$, where σ is defined to be $\gcd\{D, \frac{2N}{D}\}/2^\theta$, with θ being 1 if $2v_2(D) = v_2(N) + 1$ and 0 otherwise.

(ii) The stabilizer in $SAut^+(L(N, D))$ of the subgroup of the discriminant group which consists of images of real multiples of H (or equivalently of its orthogonal complement, inverse images of which can be taken to be spanned only by E and F over \mathbb{R}) is precisely $\Gamma_0^*(N)$.

(iii) The subgroup of $SAut^+(L(N, D))$ which fixes all the images of real multiples of H pointwise in the discriminant group is the subgroup of $\Gamma_0^*(N)$, containing $\Gamma_0(N)$, which is based only on those divisors μ of N which are co-prime to $\frac{N}{D}$.

- (iv) Elements of $SAut^+(L(N, D))$ whose action does not mix the subgroups of the discriminant group which are generated by the appropriate multiples of E , F , and H consists of those elements of $\Gamma_0^*(N)$ in which μ is co-prime to D .
- (v) The discriminant kernel of $L(N, D)$ is the subgroup Γ_H of $\Gamma_0(N)$, in which H is group consisting of those elements of $(\mathbb{Z}/N\mathbb{Z})^\times$ whose square becomes trivial in $(\mathbb{Z}/N\mathbb{Z})^\times$.

Proof. As in the proof of Lemma 4.1, we determine the $SAut^+$ group of the rescaled lattice. Similar considerations show that using the basis E , NF , and $\frac{N}{D}H$ of that lattice (rather than the generators E , NF , and NH of $\tilde{L}_0(N)$), and requiring integrality with respect to the same basis (instead of with respect to E , NF , and H spanning $L_1(N)$), we have to consider elements $A = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ of $\Gamma_0^{*,sN}(N)$ in which e^2 , $\frac{Deq}{N}$, $\frac{q^2}{N}$, $\frac{2Nef}{D}$, $eh + fg$, $\frac{2qh}{D}$, Nf^2 , Dfh , and h^2 are integers. Writing A as in Definition 1.1, we find that the numbers which must be integral are $a^2\mu$, Dac , $c^2\frac{N}{\mu}$, $\frac{2N}{D}ab$, $ad\mu + bc\frac{N}{\mu}$, $\frac{2N}{D}cd$, $b^2\frac{N}{\mu}$, Dbd , and $a^2\mu$. This is not immediate only for the expressions not involving μ , which are invariants of the matrix A (i.e., independent of the presentation) by part (i) of Lemma 1.4, and which determine the group $\Gamma_0^{*,\sigma}(N)$ to which A belongs by Remark 1.8. This determines the $SL_2(\mathbb{R})$ -pre-image of $SAut^+(L(N, D))$ as $\Gamma_0^{*,\sigma}(N)$, where σ is $\gcd\{D, \frac{2N}{D}, s_N\}$. The same considerations as in the proof of Theorem 3.1 shows that σ has the asserted value (but note the difference that here $\frac{N}{D}$ is multiplied by 2, while the number which is multiplied by 2 in that Theorem is D , whence the difference in the definition of θ). This proves part (i).

For the remaining parts it will be convenient to rescale $L^*(N, D)$ as well, to get the lattice generated by $\frac{1}{D}E$, $\frac{1}{2}H$, and $\frac{N}{D}F$ (this is *not* the dual of the rescaled lattice, but just makes the coefficients in the calculation neater). An element $A \in \Gamma_0^{*,\sigma}(N)$, written as in Definition 1.1 (or 1.7), takes this basis to

$$\frac{1}{D} \begin{pmatrix} -acN & a^2\mu \\ -c^2\frac{N^2}{\mu^2} & acN \end{pmatrix}, \quad \frac{1}{2} \begin{pmatrix} ad\mu + bc\frac{N}{\mu} & -2ab \\ 2cd & -ad\mu - bc\frac{N}{\mu} \end{pmatrix}, \quad \text{and} \quad \frac{N}{D} \begin{pmatrix} bd & -\frac{b^2}{\mu} \\ d^2\mu & -bd \end{pmatrix}$$

respectively. The parts mixing the two groups from part (ii) belong to the rescaled $L(N, D)$, i.e., are spanned by E , NF , and $\frac{N}{D}H$, if and only if ac , ab , cd , and bd are integral. This happens precisely for elements of $\Gamma_0^*(N)$ by the same argument used above, establishing part (ii). We may therefore assume, if our A is given in the form from Lemma 1.4, that a , b , c , and d are integers. Then the generator of the subgroup from part (ii) which is based on H is multiplied by the image of $ad\mu + bc\frac{N}{\mu}$ modulo $\frac{2N}{D}$, and this number is congruent to 1 modulo $\frac{2N}{\mu}$ and to -1 modulo 2μ by the SL_2 condition. As this operation on residues modulo $\frac{2N}{D}$ is via a faithful action of the quotient from part (ii) of Lemma 1.6 (with the divisor being $\frac{N}{D}$), the pointwise stabilizer of the group in question corresponds to the kernel of the projection map from that Lemma, yielding part (iii). On the other hand, the condition for elements of $\Gamma_0^*(N)$ not

to mix the group consisting of the images of multiples of E with those of F is the divisibility of $b^2 \frac{N}{\mu}$ and $c^2 \frac{N}{\mu}$ by D . But a prime dividing μ cannot divide b , c , or $\frac{N}{\mu}$, so that such divisibility condition can (and will) hold if and only if no such prime divides D , and part (iv) follows.

Now, as elements of the discriminant kernel must satisfy the conditions of both parts (iii) and (iv), and only $\mu = 1$ is co-prime to both D and $\frac{N}{D}$, we deduce from these parts that the discriminant kernel is contained in $\Gamma_0(N)$. But an element $A = \begin{pmatrix} a & b \\ Nc & d \end{pmatrix}$ of that group fixes the generator of the subgroup associated with H in the discriminant group invariant, but multiplies the generators of the groups associated with E and F by a^2 and d^2 respectively (this generalizes the assertion for $D = N$ given in Proposition 4.1 of [LZ]). As the latter subgroups are cyclic of order D , the discriminant kernel consists of those elements of $\Gamma_0(N)$ as above which satisfy the congruence $a^2 - 1 \equiv d^2 - 1 \equiv 1 \pmod{D}$. As this is precisely the asserted Γ_H , this yields part (v), hence completes the proof of the theorem. \square

The results of Proposition 2.2 of [BO] and of Remark 4.3 of [LZ] are obtained as special cases of Theorem 4.2.

Corollary 4.3. (i) *The group $SAut^+(L_0(N))$, as well as its separating subgroups from parts (ii) and (iv) of Theorem 4.2, is $\Gamma_0^*(N)$. The pointwise stabilizer of the subgroup associated with H , which is also the discriminant kernel, is just $\Gamma_0(N)$.*

(ii) *For $L_1(N)$, the $SAut^+$ group is $\Gamma_0^{*,2}(N)$ if $4|N$ and $\Gamma_0^*(N)$ otherwise. The stabilizer, as well as the pointwise stabilizer, of the group coming from H is $\Gamma_0^*(N)$. The separating subgroup from part (iv) of Theorem 4.2 is $\Gamma_0(N)$, and the discriminant kernel is $\Gamma_1^{[2]}(N)$ (or $\Gamma_1^{\sqrt{1}}(N)$ in the notation of [LZ]).*

Proof. Part (i) is the case $D = 1$ in Theorem 4.2, where multiples of E and F do not appear in the discriminant group. For part (ii) we take $D = N$ in that Theorem, so that σ from part (i) there is $\frac{\gcd\{N, 2\}}{2^\theta}$. As the numerator is 1 for odd N and $\theta = 1$ in case $v_2(N) = 1$, this proves the first assertion. The rest follows directly from Theorem 4.2, noting that the subgroup associated with H is of order 2 hence has no non-trivial automorphisms. This proves the corollary. \square

The lattice $L(N, D)$ is generated, for every N and D , by a multiple ξH with $\xi^2 \in \mathbb{N}$, together with multiples $r\xi E$ and $t\xi F$ (with rational r and t) of ξE and ξF such that the product of the total coefficients of E and F is integral. By considering all the lattices of that form we get a discriminant kernel presentation of all the groups appearing in Theorem 3.5 (up to replacing triviality modulo D by triviality of the square modulo D).

Theorem 4.4. *Take T , M , and D as in Theorem 3.5, and set $N = MT$ and σ to be $\gcd\{D, \frac{2N}{D}\}/2^\theta$, in which θ is defined to be 1 if $2v_2(D) = v_2(N) + 1$ and 0 otherwise. Then the lattice spanned by the vectors $\frac{\sqrt{DM}}{\sqrt{T}}E$, $\frac{\sqrt{DT}}{\sqrt{M}}F$,*

and $\frac{\sqrt{MT}}{\sqrt{D}}H$ has an $SAut^+$ group consisting of those matrices $\begin{pmatrix} a\sqrt{\mu} & b\frac{M}{\mu}\sqrt{\mu} \\ c\frac{T}{\mu}\sqrt{\mu} & d\sqrt{\mu} \end{pmatrix}$ for which $\begin{pmatrix} a\sqrt{\mu} & b/\sqrt{\mu} \\ c\frac{T}{\mu}\sqrt{\mu} & d\sqrt{\mu} \end{pmatrix}$ lies in $\Gamma_0^{*,\sigma}(N)$ (with μ a divisor of N with the usual properties). The group separating the discriminant images of multiples of H from those of E and F consists of those elements described above in which a, b, c , and d are integers, and the discriminant kernel is the subgroup of $\Gamma_0^0(T, M)$ in elements of which the squares of the diagonal entries are congruent to 1 modulo D .

Proof. The lattice in question is the image of $L(N, D)$ under the operation of the matrix $\frac{1}{M}\begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$, so that the required groups are obtained from those described in parts (i), (ii), and (v) of Theorem 4.2. As this yields the asserted groups, this proves the theorem. \square

Remark 4.5. Rescaling of lattices of the form $L(N, D)$, also in rational multipliers which still leave the result an even lattice (i.e., by a multiplier whose denominator divides $\gcd\{D, \frac{N}{D}\}$), yields examples of the lattices appearing in Theorem 4.4 which are not exactly $L(N, D)$. The lattices from Theorem 4.4 which arise in this way are precisely those in which the parameter M from that Theorem divides T .

As in Corollary 3.6 we obtain relations between the other congruence subgroups (up to squaring the diagonal entries) and discriminant kernels. Here is a special case of particular interest.

Corollary 4.6. *The lattice spanned by $\sqrt{M}\cdot E$, $\sqrt{M}\cdot F$, and $\sqrt{M}\cdot H$, has $SAut^+$ group $SL_2(\mathbb{Z})$, and its discriminant kernel is the group $\Gamma^{[2]}(M) = \Gamma^{\sqrt{1}}(M)$ consisting of those elements of $\Gamma_0^0(M, M)$ whose diagonal entries square to 1 modulo M . This group consists precisely of those matrices in $SL_2(\mathbb{Z})$ whose reduction modulo M is diagonal.*

Proof. This is just the case $M = N = D$ in Theorem 4.4. \square

The lattice from Corollary 4.6 is just the rescaling of $L_0(1) = L_1(1) = L(1, 1)$ by N .

All the lattices from Theorem 4.4 are isomorphic to the lattices $L(N, D)$. On the other hand, these lattices are mutually non-isomorphic.

Proposition 4.7. *Let N, M, D and C be integers such that $D|N$ and $C|M$. If $L(N, D)$ and $L(M, C)$ are isomorphic as lattices, then $M = N$ and $C = D$.*

Proof. We need to show that the isomorphism class of $L(N, D)$ determines N and D . First, $\gcd\{D, \frac{N}{D}\}$ is the minimal number M such that $L(N, D)$ is isomorphic to the rescaling of an even lattice (namely $L(\frac{N}{M^2}, \frac{D}{M})$) by M . It therefore suffices to prove the assertion for the case where D and $\frac{N}{D}$ are coprime. Now, the discriminant group is isomorphic, as an Abelian group, to the product of one cyclic group of order $\frac{2N}{D}$ (from multiples of H) and two subgroups of order D (from E and F). Hence it contains, for any prime $p|N$, a unique

subgroup of order p if $p \mid \frac{N}{D}$, but more than one such group if $p \mid D$. This allows us to determine $\frac{N}{D}$ and D , which completes the proof of the proposition. \square

We conclude with the following assertion about replacing \mathbb{R} with other fields. Let $\overline{\mathbb{Q}}$ be an algebraic closure of \mathbb{Q} (embedded in \mathbb{C} , say), and let $\mathbb{Q}(\sqrt{\mathbb{Q}})$ be the compositum of all the quadratic fields.

Proposition 4.8. (i) *The normalizer of any group Γ_H in $SL_2(\mathbb{R})$ coincides with the normalizer in $SL_2(\overline{\mathbb{Q}} \cap \mathbb{R})$, as well as with the normalizer in $SL_2(\mathbb{Q}(\sqrt{\mathbb{Q}}) \cap \mathbb{R})$.*

(ii) *The normalizers in $SL_2(\mathbb{C})$, $SL_2(\overline{\mathbb{Q}})$, and $SL_2(\mathbb{Q}(\sqrt{\mathbb{Q}}))$ also coincide. This common group is an extension of the group from part (i) by an element squaring to $-I$, having a simple action on the former group.*

(iii) *If $GL_2^{\pm 1}(\mathbb{F})$ stands, for any field \mathbb{F} , for the subgroup of GL_2 consisting of those matrices whose determinant lies in ± 1 , then the normalizer in $GL_2^{\pm 1}(\mathbb{R})$, as well as in $GL_2^{\pm 1}(\overline{\mathbb{Q}} \cap \mathbb{R})$ and in $GL_2^{\pm 1}(\mathbb{Q}(\sqrt{\mathbb{Q}}) \cap \mathbb{R})$, is another such semi-direct product.*

(iv) *The group $SAut(L(N, D))$, without the $+$ restriction, is a semi-direct product involving $SAut^+(L(N, D))$ as in part (ii). Removing the determinant restriction, the groups $Aut(L(N, D))$ and $Aut^+(L(N, D))$ are obtained as the direct product of $SAut$ (resp. $SAut^+$) with the automorphism $-Id_{L(N, D)}$ of global inversion.*

Proof. Part (i) follows directly from Proposition 2.3 and the fact that the formula from Definition 1.1 involves only square roots of non-negative rational numbers. For part (ii) we observe that one place in the proof of Proposition 2.3 where we have used the fact that our matrix has real entries is when we said that if $g = 0$ then $a = d = \pm 1$. Allowing complex (or any other algebraically closed) coefficients, we obtain also the possibility where $a = -d = \pm i$ (with $i = \sqrt{-1}$), yielding just real matrices multiplied by $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. The only other place in that proof where reality was used is where the number t was assumed to be positive. As allowing t to be negative is the same as multiplying a matrix from $SL_2(\mathbb{R})$ by $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ as well, we find that the group in question contains the normalizer as a subgroup of index 2, with which $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ generates the full group. As this matrix squares to the non-trivial central element $-I$ of the real normalizer, and conjugation by which simply inverts the signs of the off-diagonal entries, this proves part (ii). Part (iii) is easily deduced by replacing $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ by its real counterpart $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, which has determinant -1 and order 2, and conjugation by which yields the same operation as in part (ii). For part (iv) we recall that conjugation by matrices of determinant -1 yields the operation of elements $SO(M_2(\mathbb{R})_0)$ which do not preserve the orientations on the definite parts (e.g., the matrix from the proof of part (iii) preserves the positive norm vector $E - F$, but inverts the vectors $E + F$ and H , of norms -2 and 2 respectively). Hence the first assertion follows from part (iii), and the second one is a consequence of the fact that

$-Id_{L(N,D)}$ is central, has determinant -1 , and preserves the orientation on the 2-dimensional positive definite part. This proves the proposition. \square

We conclude with remarking that part (iv) of Proposition 4.8 considers only two intermediate groups between $Aut(L(N,D))$ and $SAut^+(L(N,D))$. The remaining group, which is defined by preserving the orientation on the negative definite part, is canonically isomorphic to $SAut(L(N,D))$. The isomorphism leaves $SAut^+(L(N,D))$ invariant and multiplies every element of $SAut(L(N,D)) \setminus SAut^+(L(N,D))$ by $-Id_{L(N,D)}$. In addition, we have allowed only determinants ± 1 in part (iii) of Proposition 4.8 and only determinant 1 in part (ii) there since we are only interested in groups whose center consists just of $\{\pm I\}$ (otherwise the center just enters all the normalizers, and increases them trivially).

References

- [AL] Atkin, A. O. L., Lehner, J., HECKE OPERATORS ON $\Gamma_0(m)$, Math. Ann., vol 185, 134–160, (1970).
- [AS] Akbas, M., Singerman, D., THE NORMALIZER OF $\Gamma_0(N)$ IN $PSL_2(\mathbb{R})$, Glasgow Math. J., vol 32 no. 3, 317–327, (1990).
- [B] Bars, F., THE GROUP STRUCTURE OF THE NORMALIZER OF $\Gamma_0(N)$ AFTER ATKIN–LEHNER, Communications in Algebra, vol 36 no. 6, 2160–2170 (2008)
- [BO] Bruinier, J. H., Ono, K., HEEGER DIVISORS, L -FUNCTIONS, AND HARMONIC WEAK MAASS FORMS, Ann. of Math., vol 172, 2135–2181 (2010).
- [C] J. H. Conway, UNDERSTANDING GROUPS LIKE $\Gamma_0(N)$, in “Groups, Difference Sets, and the Monster (Columbus, OH, 1993)”, Ohio State Univ. Math. Res. Inst. Publ., Vol. 4, de Gruyter, Berlin (1996).
- [CN] Conway, C., Norton, S., MONSTROUS MOONSHINE, Bull. London Math. Soc., vol 11, 308–339 (1979).
- [DS] Diamond, F., Shurman, J., A FIRST COURSE IN MODULAR FORMS, Graduate Texts in Mathematics 228, Springer-Verlag, New York (2005).
- [L1] Lang, M. L., NORMALISER OF $\Gamma_1(m)$, J. Number Theory, vol 86, 50–60, (2001).
- [L2] Lang, M. L., NORMALIZERS OF THE CONGRUENCE SUBGROUPS OF THE HECKE GROUPS G_4 AND G_6 , J. Number Theory, vol 90 issue 1, 31–43, (2001).
- [L3] Lang, M. L., NORMALISERS OF SUBGROUPS OF THE MODULAR GROUP, J. Algebra, vol 248, 202–218, (2002).
- [LN] Lehner, J., Newman, M., WEIERSTASS POINTS OF $\Gamma_0(n)$, Ann. Math., vol 79 no. 2, 360–368, (1964).

- [LZ] Li, Y., Zemel, S., SHIMURA LIFTS OF WEAKLY HOLOMORPHIC MODULAR FORMS, preprint.
- [N1] Newman, M., THE NORMALIZER OF CERTAIN MODULAR SUBGROUPS, Canad. J. Math., vol 8, 29–31, (1956).
- [N2] Newman, M., NORMALIZERS OF MODULAR GROUPS, Math. Ann., vol 238 issue 2, 123–129, (1978).

EINSTEIN INSTITUTE OF MATHEMATICS, THE HEBREW UNIVERSITY OF JERUSALEM,
EDMUND SAFRA CAMPUS, JERUSALEM 91904, ISRAEL
E-mail address: zemels@math.huji.ac.il